Europ. J. Combinatorics (2001) **22**, 455–464
doi:10.1006/eujc.2000.0471
Available online at http://www.idealibrary.com on IDEAL®

Sets with few Intersection Numbers from Singer Subgroup Orbits

J. COYKENDALL AND J. DOVER

Using a Singer cycle in Desarguesian planes of order $q \equiv 1 \pmod 3$, q a prime power, Brouwer [2] gave a construction of sets such that every line of the plane meets them in one of three possible intersection sizes. These intersection sizes x, y, and z satisfy the system of equations

$$x + y + z = q + 1$$
$$x^2 + y^2 + z^2 = \frac{1}{3}(q^2 + 4q + 1).$$

Brouwer claimed that this system has a unique solution in integers. Further, Brouwer noted that for q a perfect square, this system has a solution for which two of the variables are equal, ostensibly implying that when q is a square the constructed set has only two intersection numbers.

In this paper, we perform a detailed analysis which shows that this system does not in general have a unique solution. In particular, the constructed sets when q is a square might have three intersection numbers. The cases for which this occurs are completely determined.

1. INTRODUCTION

Let π be a projective plane of order q. A set S of points in π is said to be of *type* $(a_0, \ldots, a_k)$ if for every line there exists an i such that the line meets S in a_i points, and for each a_i, some line meets S in a_i points. The numbers a_i are called the *intersection numbers* of the set. Of particular interest are sets which have few intersection numbers. The most studied sets are those with only two intersection numbers, and not much seems to be known in the general case of sets with more than two; see Hirschfeld [7] for a survey of known results.

Of particular interest to us here is a construction due to Brouwer [2] of sets with three intersection numbers. Let $q \equiv 1 \pmod 3$ be a prime power. The Desarguesian projective plane of order q (hereafter denoted as $PG(2, q)$) can be modelled as a three-dimensional vector space over $GF(q)$ with homogeneous coordinates. We may take this vector space to be $V = GF(q^3)$, and we will let β denote a primitive element of this field. The points of $PG(2, q)$ are the one-dimensional subspaces of V; since we are working with homogeneous coordinates, each point may be represented as the span of one of $1, \beta, \ldots, \beta^{q^2+q}$. When no ambiguity can occur, we will simply refer to a point by one of these field elements. The lines of $PG(2, q)$ are the two-dimensional subspaces of V, and the lines may similarly be referred to by field elements $1, \beta, \ldots, \beta^{q^2+q}$; here the line indexed by field element k corresponds to the set of points

$$\{\beta^i | i \in \{0, \ldots, q^2 + q\} \text{ and } \mathrm{Tr}(k\beta^i) = 0\},$$

where Tr is the trace function from $GF(q^3)$ to $GF(q)$, i.e., $\mathrm{Tr}(k) = k + k^q + k^{q^2}$.

A *Singer cycle* is a mapping which cyclically permutes the points and cyclically permutes the lines of $PG(2, q)$. It is not difficult to see that the mapping $\Sigma : k \mapsto \beta k$ induces a Singer cycle σ on $PG(2, q)$. (Of course, β^{q^2+q+1} is a $GF(q)$-multiple of β^0, so maintaining our above representation of points and lines requires one to reduce exponents modulo q^2+q+1.)

Note that the group generated by a Singer cycle has order $q^2 + q + 1$, which in the case $q \equiv 1 \pmod 3$ is divisible by three. Let S be the group which is generated by σ^3. Then S possesses three point orbits and three line orbits, each of size $1/3(q^2 + q + 1)$. Let A_0, A_1,

0195–6698/01/040455 + 10 $35.00/0

and A_2 denote these point orbits, and L_0, L_1, and L_2 denote the line orbits. More explicitly

$$A_i = \left\{ \beta^{3j+i} \mid j \in \left\{ 0, \ldots, \frac{1}{3}(q^2+q+1) - 1 \right\} \right\}. \tag{1}$$

Let ℓ be a line of L_0. Suppose ℓ meets A_0 in x points, A_1 in y points, and A_2 in z points. It is easy to see that σ maps A_0 onto A_1, A_1 onto A_2, and A_2 onto A_0. A similar action on lines will be assumed (by relabelling, if necessary).

Let m denote the image of ℓ under σ; by definition m is a line in orbit L_1. Since σ cyclically permutes our point orbits, we conclude that m meets A_0 in z points, A_1 in x points, and A_2 in y points. Using this logic, it is not difficult to show that every line in orbit L_0 meets A_0 in x points, A_1 in y points, and A_2 in z points; every line of orbit L_1 meets A_0 in z points, A_1 in x points, and A_2 in y points; and every line of orbit L_2 meets A_0 in y points, A_1 in z points, and A_2 in x points. Further, the ordering of x, y, and z is not arbitrary. In any Desarguesian plane of order $q \equiv 1 \pmod 3$ with any Singer cycle σ, there will be a labelling of the point and line orbits under σ^3 which have exactly these intersection patterns and cyclic action under σ.

Using straightforward counting arguments, Brouwer [2] determined that the intersection numbers x, y, and z satisfy the system

$$\begin{aligned} x + y + z &= q + 1 \\ x^2 + y^2 + z^2 &= \frac{1}{3}(q^2 + 4q + 1). \end{aligned} \tag{2}$$

We note that the intersection numbers need not be distinct, but this can occur only if q is a perfect square, in which case the intersection numbers must be

$$\begin{aligned} x = y &= \frac{1}{3}(q \pm \sqrt{q} + 1) \\ z &= \frac{1}{3}(q \mp 2\sqrt{q} + 1), \end{aligned}$$

where signs are determined by the requirement that these quantities be integers.

Brouwer [2] erroneously claimed that the system of Eqns (2) has a unique (up to ordering of the variables) solution in integers. From this assertion, it followed that when q is a square, the constructed sets have only two intersection numbers.

In the following section, we show that this system does not in general have a unique solution. We then proceed to analyze the sets in $PG(2, q)$ with q a square and show that under certain conditions these sets do NOT have just two intersection numbers.

2. A Diophantine Analysis

We now wish to analyze the system of Eqns (2) solely as a system of Diophantine equations, forgetting for the moment the ambient geometry. Before we manipulate the above equations, we need a few lemmas concerning a particular quadratic norm form (that is, a quadratic form that arises from the norm of an order in a quadratic field).

LEMMA 2.1. *The quadratic forms $x^2 - xy + y^2$ and $x^2 + 3y^2$ represent the same set of integers.*

PROOF. We note that the first quadratic form is the norm arising from the quadratic ring of integers $\mathbb{Z}[\omega]$, where $\omega = \frac{-1-\sqrt{-3}}{2}$ is a primitive cube root of unity. The second quadratic form arises as the norm of the subring $\mathbb{Z}[\sqrt{-3}]$. In [4] it was shown that the rings $\mathbb{Z}[\omega]$ and $\mathbb{Z}[\sqrt{-3}]$ possess the same normset and this is exactly the claim of this lemma. □

LEMMA 2.2. *If $\alpha \in \mathbb{Z}[\omega]$ is prime to 2, then precisely one of the units (say u) in the set $\{1, \omega, \omega^2\}$ is such that $u\alpha \in \mathbb{Z}[\sqrt{-3}]$.*

PROOF. The previous lemma can be applied to give existence, so without loss of generality, we shall assume that $\alpha = x + y\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$. Assume that $\omega\alpha \in \mathbb{Z}[\sqrt{-3}]$. A simple computation shows that x and y must be of the same parity. Hence $N(\alpha) = x^2 + 3y^2$ must be even, so α is not prime to 2. The proof for ω^2 is the same. □

LEMMA 2.3. *Let p be a prime integer and $q = p^n$ with $n \geq 1$. The number (m) of distinct solutions to the equation $x^2 + 3y^2 = q$ is given by:*

$$m = \begin{cases} 2n + 2, & \text{if } p \equiv 1 \pmod 3; \\ 1 + (-1)^n, & \text{if } p \equiv 2 \pmod 3,\ p \neq 2; \\ 3(1 + (-1)^n), & \text{if } p = 2. \end{cases}$$

PROOF. We first note that an elementary computation shows that in the ring $\mathbb{Z}[\omega]$, the rational prime p splits into two distinct factors if $p \equiv 1 \pmod 3$ and is inert (remains prime) if $p \equiv 2 \pmod 3$. We will ignore the ramified case ($p = 3$).

We first consider the case where $p \equiv 1 \pmod 3$. In this case, we write

$$p = \alpha_1\alpha_2,$$

where α_1 and α_2 are primes in $\mathbb{Z}[\omega]$. Since $\mathbb{Z}[\omega]$ is a UFD, the above factorization of p is unique up to inserting units. The proof of Lemma 2.1 shows that there are units in $u_1, u_2 \in \mathbb{Z}[\omega]$ such that $u_1\alpha_1, u_2\alpha_2 \in \mathbb{Z}[\sqrt{-3}]$. Hence we will assume that α_1 and α_2 are already in $\mathbb{Z}[\sqrt{-3}]$.

Searching for solutions to $x^2 + 3y^2 = p^n$ is equivalent to searching for solutions to the equation $N(\beta) = p^n$ where $\beta = x + y\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}[\omega]$ and N denotes the standard norm map.

We first consider the equation in $\mathbb{Z}[\omega]$

$$N(\beta) = (\beta)(\overline{\beta}) = p^n,$$

where $\overline{\beta}$ denotes the conjugate of β. As $\mathbb{Z}[\omega]$ is a UFD we can factor $p^n = (\alpha_1)^n(\alpha_2)^n$ uniquely up to units; hence we deduce that

$$\beta = \prod_{i=1}^{n} \gamma_i,$$

where up to units, each γ_i is either α_1 or α_2. However, since p^n is prime to 2, we apply Lemma 2.2 and assert that, in fact, we can assume that each γ_i is precisely $\pm\alpha_1$ or $\pm\alpha_2$.

We now consider ways to construct solutions to the equation $N(\beta) = p^n$ in $\mathbb{Z}[\sqrt{-3}]$. The previous argument shows that any such solution is of the form

$$\beta = \pm(\alpha_1)^m(\alpha_2)^{n-m},$$

where $0 \leq m \leq n$. The fact that both α_1 and α_2 are prime in $\mathbb{Z}[\omega]$ (and in $\mathbb{Z}[\sqrt{-3}]$) shows that each value of m gives a distinct solution to the norm equation. Hence we merely count to find that there are precisely $2(n + 1)$ distinct solutions.

The case where $p \equiv 2 \pmod 3$ is an even easier application of this technique, only care must be taken for the case $p = 2$. The important difference being that now all the elements $\{2, 2\omega, 2\omega^2\}$ are elements of $\mathbb{Z}[\sqrt{-3}]$. Effectively, the case $p = 2$ has three times the number of solutions of the case $p \equiv 2 \pmod 3$, $p > 2$. □

With these tools in hand, we now proceed to the main result of this section, which shows that the system of Eqns (2) does not have a unique solution when $p \equiv 1 \pmod 3$ for $q = p^e$.

THEOREM 2.4. *Consider the system of Diophantine equations*

$$x + y + z = q + 1$$
$$x^2 + y^2 + z^2 = \frac{1}{3}(q^2 + 4q + 1),$$

where $q = p^n$ is a prime power. The number, m, of distinct solutions to this system is given by

$$m = \begin{cases} \frac{2n+3+(-1)^n}{4}, & \text{if } p \equiv 1 \pmod 3; \\ \frac{1+(-1)^n}{2}, & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Moreover, $x, y, z \geq 0$.

PROOF. The nonnegativity of x, y and z for any solution to our system is an easy exercise. Note that our system of equations is symmetric in the variables x, y, and z and we ignore multiple solutions that arise as permutations of a given solution.

To begin, we will rewrite the above system in a more convenient form. Without loss of generality, we assume that we have chosen x and y of the same parity. Solving for z and implementing the change of variables

$$x \mapsto X + Y$$
$$y \mapsto X - Y,$$

we reduce to the equation

$$Z^2 + 3Y^2 = A - 1 = q,$$

where $Z = 3X - A$.

At this juncture, we note that Lemma 2.3 shows that our system must have no solutions in the case that n is odd and $p \equiv 2 \pmod 3$. Assuming that this is not the case (that is we have found a solution (Z, Y)), it is easy to see that a solution to our original system is given by

$$x = \frac{A + Z}{3} + Y$$
$$y = \frac{A + Z}{3} - Y$$
$$z = \frac{A - 2Z}{3}.$$

Note that given any solution (Z, Y) to the equation $Z^2 + 3Y^2 = q$ we actually have four (two if $Y = 0$) distinct solutions $(\pm Z, \pm Y)$. Note that since Z is not divisible by 3, we see that only one of $\pm Z$ produces an integral answer for x and y. We also note that altering the sign of Y results only in interchanging the roles of x and y in the above solution. Hence every collection of four solutions (respectively, two solutions) $(\pm Z, \pm Y)$ collapses to one solution of our Diophantine system.

Applying Lemma 2.3, we see that for the case $p \equiv 1 \pmod 3$, there are $2n + 2$ solutions to the equation $Z^2 + 3Y^2 = p^n$. By grouping solutions together if they vary only by signs, we partition them into $\frac{2n+2}{4}$ subsets if n is odd and $\frac{2n+4}{4}$ subsets if n is even. The arguments for $p \equiv 2 \pmod 3$ are similar.

It only remains to show that when $p \equiv 1 \pmod 3$ all of the enumerated solutions actually correspond to distinct solutions to our original system.

Consider two distinct solutions (Z_1, Y_1) and (Z_2, Y_2) to the equation $Z^2 + 3Y^2 = q$. We write the solutions to our Diophantine system

$$x_1 = \frac{A + Z_1}{3} + Y_1$$
$$y_1 = \frac{A + Z_1}{3} - Y_1$$
$$z_1 = \frac{A - 2Z_1}{3},$$

and

$$x_2 = \frac{A + Z_2}{3} + Y_2$$
$$y_2 = \frac{A + Z_2}{3} - Y_2$$
$$z_2 = \frac{A - 2Z_2}{3}.$$

Assume that these solutions are rearrangements of each other. If $z_1 = z_2$ then it is easy to see that $Z_1 = Z_2$ and hence $Y_1 = \pm Y_2$ so we ignore this case.

Without loss of generality, we assume that $x_1 = x_2$ (note x_1 can be chosen to be either x_2 or y_2 and for convenience we assume x_2 since x_2 and y_2 differ only by the choice of the square root of Y^2). Thus we conclude from the above remark that $y_1 = z_2$ and $z_1 = y_2$. This gives rise to the following equations

$$Z_1 + 3Y_1 = Z_2 + 3Y_2$$
$$Z_1 - 3Y_1 = -2Z_2$$
$$-2Z_1 = Z_2 - 3Y_2.$$

Combining the first two equations gives $2Z_1 = -Z_2 + 3Y_2$. Reducing this equation modulo 2, we see that Z_2 and Y_2 must be of the same parity. Hence $Z_2^2 + 3Y_2^2 = 2^k$ which is a contradiction. This establishes the theorem. □

This algebraic approach demonstrates why uniqueness fails to hold for $p \equiv 1 \pmod 3$ for integers $n > 1$; however, all solutions can be examined as they are generated by the unique solution for the case $n = 1$.

3. The Situation for Square q

In this section q is of the form p^{2n} unless explicitly stated otherwise. We would like to prove the following theorem.

THEOREM 3.1. *In $PG(2, q)$, where $q = p^{2n} \equiv 1 \pmod 3$, let A_0 be defined as in Eqn* (1). *If $p \equiv 2 \pmod 3$, then A_0 has exactly two intersection numbers. If $p \equiv 1 \pmod 3$, then A_0 has exactly three intersection numbers.*

The proof of the first assertion follows directly from Theorem 2.4. We know A_0 has at most three intersection numbers x, y, and z, which satisfy the system of Eqns (2). When

$p \equiv 2 \pmod 3$, Theorem 2.4 states that the system of Eqns (2) has only one solution, and from the discussion in Section 1, we know that this solution has two of the intersection numbers equal, yielding just two distinct intersection numbers.

We now tackle the situation where $p \equiv 1 \pmod 3$. The analysis here is much more intricate, requiring us to delve into the geometry of Singer cycles.

Consider the collineation $\sigma : x \mapsto \beta x$ of $PG(2, q)$ from Section 1. Note that if q is a square, the order of σ factors as $q^2 + q + 1 = (q + \sqrt{q} + 1)(q - \sqrt{q} + 1)$. This factorization gives rise to the following geometric structures associated with orbits under subgroups of σ. (See Bruck [3], Borós and Szönyi [1], and Fisher *et al*. [6] for details and proofs.)

The subgroup generated by $\sigma^{q+\sqrt{q}+1}$ has $q + \sqrt{q} + 1$ point orbits of size $q - \sqrt{q} + 1$. These orbits are complete arcs (in particular, no line meets an arc in more than two points) and can be described as

$$\mathrm{A}(t) = \{\beta^{t+i(q+\sqrt{q}+1)} | i \in \{0, \ldots, q - \sqrt{q}\}\} \tag{3}$$

for every $t \in \{0, \ldots, q + \sqrt{q}\}$. These arcs partition $PG(2, q)$, and the collection of these arcs will be called the *standard arc partition*, and be denoted $\mathcal{A}$.

On the other hand, the subgroup generated by $\sigma^{q-\sqrt{q}+1}$ has $q - \sqrt{q} + 1$ point orbits of size $q + \sqrt{q} + 1$. These orbits are Baer subplanes (i.e., copies of $PG(2, \sqrt{q})$) of $PG(2, q)$, and they can also be described algebraically via

$$\mathrm{B}(t) = \{\beta^{t+i(q-\sqrt{q}+1)} | i \in \{0, \ldots, q + \sqrt{q}\}\}$$

for each $t \in \{0, \ldots, q - \sqrt{q}\}$. Again, these Baer subplanes partition the points of $PG(2, q)$, and the collection of these subplanes will be denoted $\mathcal{B}$ and be called the *standard Baer subplane partition*.

In addition to these structures, one also gets Hermitian unitals into the picture. (A Hermitian unital, i.e., a classical unital, is the set of absolute points of a unitary polarity.) Borós and Szönyi [1], and independently Fisher *et al*. [6] proved that the sets

$$\mathrm{U}(a) = \{x | \mathrm{Tr}(ax^{q\sqrt{q}+1}) = 0\} \tag{4}$$

are Hermitian unitals whenever $a \in \mathrm{B}(0)$; it is straightforward to show that $\mathrm{U}(a) = \mathrm{U}(a')$ if and only if a and a' are $GF(q)$-multiples of each other. (Note: Tr again denotes the trace function from $GF(q^3)$ to $GF(q)$.) Further, each of these unitals is partitioned into $\sqrt{q} + 1$ of the arcs $\mathrm{A}(t)$.

Our first task is to develop an embedding of $PG(2, \sqrt{q})$ in $PG(2, q)$; we note that this embedding has been discussed implicitly in Fisher *et al*. [6], but would like to revisit some of the details here.

Fisher *et al*. [6] proved that each Hermitian unital $\mathrm{U}(a)$ of Eqn (4) meets B(0) in a conic of B(0) for q odd. Further, if we take as points the points of B(0) and as 'lines' the set of conics $\mathrm{B}(0) \cap \mathrm{U}(a)$ as a varies over the field elements representing points of B(0), the resulting incidence structure is a copy of $PG(2, \sqrt{q})$. (Such a set of conics in a projective plane is often called a *projective bundle*.) For us, there is a more useful way to think of this projective bundle, which we call $\mathcal{P}$. Note that each arc of the standard arc partition meets B(0) in a unique point, and that each of the Hermitian unitals $\mathrm{U}(a)$ either contains or is disjoint from any arc of this partition. We wish to create an incidence structure Π via:

- Points of Π: the arcs of the standard arc partition.
- Lines of Π: the Hermitian unitals $\mathrm{U}(a)$.
- Incidence: containment.

Construct a mapping Φ which sends a point of B(0) onto the unique arc of the standard arc partition which contains it and which maps a conic of $\mathcal{P}$ onto the Hermitian unital U(a) containing it. Φ gives an isomorphism from the projective plane induced by our projective bundle $\mathcal{P}$ onto the incidence structure Π, which shows that Π is isomorphic to $PG(2, \sqrt{q})$.

An important point to note is that the group generated by $\sigma^{q-\sqrt{q}+1}$ acts as a Singer cycle on Π, as this group cyclically permutes the arcs of the standard arc partition. In addition, this group leaves each Baer subplane of $\mathcal{B}$ invariant, and acts on each of these Baer subplanes as a Singer cycle.

We can now give our strategy. We wish to determine how any given line ℓ of $PG(2, q)$ meets our point orbits A_0, A_1, and A_2. Since each of these point orbits is a union of arcs from the standard arc partition, we can consider these orbits as sets of points in our incidence structure Π. Since the group generated by σ acts as a Singer cycle on Π, it is not difficult to see that the set of points corresponding to A_0 in Π is exactly a point orbit under an index three subgroup of a Singer cycle, i.e., this is exactly the type of set we are considering, but in a lower order plane. Hence we can potentially use information about our sets in the lower order plane Π to obtain some information in $PG(2, q)$. In order to effectively use this correspondence, we must first discover how the lines of $PG(2, q)$ interact with Π. We begin with a lemma that describes the set of arcs in the standard arc partition which meet a given line in just one point.

LEMMA 3.2. *Let $q > 2$ be a prime power, and let ℓ be any line of $PG(2, q)$. Then ℓ is tangent to the arcs of $\mathcal{A}$ which contain the points of $\ell \cap B$, where B is the unique Baer subplane of the standard Baer subplane partition $\mathcal{B}$ having ℓ as a line.*

PROOF. This result is a simple consequence of Theorem 3.4 in Fisher *et al.* [6]. □

We now use Lemma 3.2 to prove a lemma which describes the structure of the set of Hermitian unitals U(a) to which a line ℓ is tangent.

LEMMA 3.3. *Let $q > 2$ be an odd prime power, and let ℓ be a line of $PG(2, q)$. Then ℓ is tangent to exactly $\sqrt{q} + 1$ Hermitian unitals* U(a) *from Eqn* (4)*, and these Hermitian unitals are exactly the ones such that their intersection with B meets ℓ in just one point, where B is the unique Baer subplane of $\mathcal{B}$ having ℓ as a line.*

PROOF. Let ℓ be any line of Π. Letting x denote the number of Hermitian unitals from Eqn (4) to which ℓ is tangent, and y the number which meet ℓ in $\sqrt{q} + 1$ points, we find the following relationships:

$$x + y = q + \sqrt{q} + 1$$
$$x + (\sqrt{q} + 1)y = (\sqrt{q} + 1)(q + 1).$$

The first equation comes from counting the number of Hermitian unitals of Eqn (4). The second comes from counting pairs of the form (P, U), where P is a point of ℓ and U is a Hermitian unital of the required form. Solving the system of equations above shows that $x = \sqrt{q} + 1$ and $y = q$.

For ℓ to be tangent to a Hermitian unital U(a), ℓ must be tangent to a single arc from $\mathcal{A}$ which is contained in U(a). By Lemma 3.2 this implies that ℓ must meet the conic $B \cap$ U(a) in a single point. It is an easy exercise to show that there are exactly $\sqrt{q} + 1$ Hermitian unitals U(a) for which this is true, proving the result. □

We can now state a theorem which will be our main tool for extracting information about $PG(2, q)$ from Π.

THEOREM 3.4. *Let $q > 2$ be an odd prime power, and let ℓ be a line of $PG(2, q)$. The set of arcs in $\mathcal{A}$ to which ℓ is tangent form a conic in the incidence structure Π. The exterior points of this conic in Π are exactly the arcs of $\mathcal{A}$ which do not meet ℓ, and the interior points of this conic are exactly the arcs of $\mathcal{A}$ which meet ℓ in two points.*

PROOF. Let B be the unique Baer subplane of $\mathcal{B}$ for which ℓ is a line. Note that the group generated by $\sigma^{q+\sqrt{q}+1}$ cyclically permutes the Baer subplanes of $\mathcal{B}$ and leaves each arc of $\mathcal{A}$ invariant. By taking the image of ℓ under the appropriate element of this group, we may assume without loss of generality that B is the subplane B(0).

By Lemma 3.2, we know that each arc of $\mathcal{A}$ to which ℓ is tangent meets ℓ in a point of B; this set of points forms a line of $PG(2, \sqrt{q})$. Since a line and a conic meet in at most two points, this set of points forms a $(\sqrt{q}+1)$-arc in the projective plane induced by the projective bundle $\mathcal{P}$. Since Segré's theorem implies that every $(\sqrt{q}+1)$-arc in $PG(2, \sqrt{q})$ for q odd is a conic, we can use our isomorphism Φ from the plane induced by the projective bundle $\mathcal{P}$ onto Π, and we find that the set of arcs in $\mathcal{A}$ to which ℓ is tangent forms a conic C in Π.

From Lemma 3.3 we know that the Hermitian unitals U(a) to which ℓ is tangent are exactly those such that the conic B(0) $\cap$ U(a) meets ℓ in just one point. Again using our isomorphism Φ, these unitals are exactly the tangent lines to the conic C in Π. Since ℓ is tangent to these Hermitian unitals which are tangent to C, it follows that the exterior points to C in Π are arcs of $\mathcal{A}$ which do not meet ℓ. Simple counting then shows that the interior points of C in Π correspond to arcs of $\mathcal{A}$ which meet ℓ in two points. □

The importance of this result is the following. Given a set S in $PG(2, q)$ which is the union of pairwise disjoint arcs of $\mathcal{A}$, Theorem 3.4 states that we can calculate the intersection sizes of any line with S by looking at the conic induced by that line in the incidence structure Π, and computing the number of conic points plus twice the number of interior points which correspond to arcs in S. This is exactly what we propose to do for our point orbits A_0, A_1, and A_2 in the following theorem.

THEOREM 3.5. *Let $q = p^e$ where $p \equiv 1 \pmod 3$. Let σ be a Singer cycle of the plane $PG(2, q)$ and let A_0 be a point orbit under the group generated by σ^3. Then A_0 has three distinct intersection numbers.*

PROOF. Note that q can be written as $q = p^{2^i r}$ for some integers i and r, with r odd. Our proof is by induction on i; note that the base case $i = 0$ is trivial, for in this case q is not a square, and the system of Eqns (2) has no solution with just two intersection numbers.

Suppose now the result is true for $q' = p^{2^{i-1} r}$, and note that $q' = \sqrt{q}$. Let A_0, A_1, and A_2 denote the point orbits of $PG(2, q)$ under σ^3, and let τ denote $\sigma^{q-\sqrt{q}+1}$. As we have noted above, the group generated by τ acts as a Singer cycle on Π, our incidence structure of arcs and Hermitian unitals.

As previously noted each of A_0, A_1, and A_2 is the union of arcs in $\mathcal{A}$. Hence we may consider each of A_0, A_1, and A_2 as a set of points in Π; we will refer to these sets of points in Π as P_0, P_1, and P_2. Note that P_0, P_1, and P_2 are the point orbits of Π under τ^3. In a similar manner, the lines of Π break up into three line orbits under τ^3, which we refer to as L_0, L_1, and L_2. As in the introduction, there exist constants x, y, and z dependent only on $\sqrt{q}$ such that the lines of L_0 meet P_0 in x points, P_1 in y points, and P_2 in z points; the lines in class L_1 meet P_0 in z points, P_1 in x points, and P_2 in y points; and the lines of class L_2 meet P_0 in y points, P_1 in z points, and P_2 in x points. These constants satisfy the system of Eqns (2) (with q replaced by $\sqrt{q}$), and are distinct by our induction hypothesis.

For each line ℓ, we wish to determine the number of points of A_0 that ℓ contains. Noting again that the group generated by $\sigma^{q+\sqrt{q}+1}$ leaves each arc of $\mathcal{A}$ invariant while cyclically

permuting the Baer subplanes of $\mathcal{B}$, every line ℓ has the exact same intersection pattern with the arcs in $\mathcal{A}$ as any other line in ℓ's orbit under this group. Thus we may without loss of generality look at just the lines of B(0).

From the proof of Theorem 3.4, the set of lines in B(0) give rise to a set of conics $\mathcal{Q}$ in Π, and it is not difficult to see that this set of conics is a projective bundle. Further, since the group generated by τ acts as a Singer cycle on B(0), it also acts as a Singer cycle on the projective bundle $\mathcal{Q}$. We may thus look at the action of τ^3 on the points and 'lines' of the projective plane induced by $\mathcal{Q}$; the point orbits are exactly the sets P_0, P_1, and P_2, and the 'lines' will break up into three orbits as with the lines of Π. By looking at this situation in Π, we find that $\mathcal{Q}$ breaks up into three classes Q_0, Q_1, and Q_2 with the property that every conic meets P_0 in one of x, y, or z points and τ maps Q_0 onto Q_1, Q_1 onto Q_2, and Q_2 onto Q_0. If we let Q_0 be the set of conics which meet P_0 in x points, then it follows that every conic of Q_0 meets P_0 in x points, P_1 in y points, and P_2 in z points; every conic of Q_1 meets P_0 in z points, etc.

From Theorem 3.4, we know that we can determine the intersection numbers of our original sets A_0, A_1, and A_2 by determining the number of conic points and number of interior points of a conic in $\mathcal{Q}$ which lie on the sets P_0, P_1, and P_2; the previous paragraph gives us an indication of how to count the former of these quantities. We now need to develop some tools to do the latter. The key is to consider the set of tangent lines (i.e., a *dual conic*) to one of the conics in $\mathcal{Q}$. It is not difficult to see that we could have worked dually through all of the proceeding discussion; in particular, this implies that if we consider the incidence structure whose points are the lines of Π, and whose lines are the dual conics to the conics in $\mathcal{Q}$, we would again obtain an isomorphic copy of $PG(2, \sqrt{q})$, with τ again acting as a Singer cycle on this plane. Again using the above ideas, we find that there are three orbits of 'points' under τ^3; these are exactly the line orbits L_0, L_1, and L_2. The dual conics to conics in $\mathcal{Q}$ also fall into three orbits, which we refer to as D_0, D_1, and D_2, with the usual assumption that τ maps D_0 onto D_1, etc. In particular, this implies that the same analysis we performed above to determine how the conics in $\mathcal{Q}$ met the sets P_0, P_1, and P_2 will apply to determining how lines of D_0, D_1, and D_2 are partitioned among L_0, L_1, and L_2.

Let C be a conic of class Q_0. Let us assume for the moment that the dual conic to C lies in class D_0. C meets P_0 in x points. C has x tangents of type L_0, which meet P_0 in x points, y tangents of type L_1 which meet P_0 in z points, and z tangents of type L_2 which meet P_0 in y points. Each exterior point to C lies on two tangents to C while each conic point of C lies on just one tangent. This implies that the number of exterior points to C in P_0 is $\frac{1}{2}(x^2+2yz-x)$. Hence the number of interior points to C on P_0 is $\frac{1}{3}(q+\sqrt{q}+1)-x-\frac{1}{2}(x^2-x+2yz)$. Thus from Theorem 3.4, we know that any line of $PG(2,q)$ which gives rise to the conic C in Π meets A_0 in $x+2u-\frac{1}{2}(x^2+x+2yz) = 2u-x^2-2yz$, where we define u to be $\frac{1}{3}(q+\sqrt{q}+1)$; similar counts show that such a line meets A_1 in $2u-z^2-2xy$ points and A_2 in $2u-y^2-2xz$ points.

By way of contradiction, suppose two of these intersection numbers are equal; since the equations are symmetric, we may assume without loss of generality that $2u-x^2-2yz = 2u-z^2-2xy$. This equation can be easily manipulated to obtain $x^2-z^2 = 2y(x-z)$. We know x and z are distinct by our induction hypothesis, so we must have $2y = x+z$. Using the system of Eqns (2) (with $\sqrt{q}$ substituted for q), we find that $3y = \sqrt{q}+1$. However, by assumption $\sqrt{q} \equiv 1 \pmod 3$, which contradicts the fact that y is an integer. Hence the point orbits A_0, A_1, and A_2 have three distinct intersection numbers.

It is not difficult to repeat the above counts for the cases where the dual conic to C is in class D_1 or D_2. We merely point out that the exact same intersection numbers arise in these two cases. This finishes the proof. □

4. Conclusion

While we have been unable to give a formula for the exact solutions of our system of Diophantine Eqns (2), we have been able to determine enough information to show that they do not tell the entire story in this case, as was suspected by Brouwer. The geometric techniques we have developed allow us to clarify the situation, and we now know when our sets truly have just two intersection numbers. We feel, however, that the geometric techniques used have much broader potential application.

We wish to close with a fundamental problem related to sets with two intersection numbers upon which the methods used here may prove useful. For a putative set of type (m, n) in a plane of order q, there exist many algebraic constraints on the values of m and n (see Hirschfeld [7]). However for any square q, the pair $(a, \sqrt{q}+a)$ always satisfies the constraints; however, the putative sets must have size either $a(q + \sqrt{q} + 1)$ or $(\sqrt{q} + a)(q - \sqrt{q} + 1)$. De Finis [5] has shown that sets of the former size always exist, and can be constructed as the union of pairwise disjoint Baer subplanes. The combinatorics of the latter size strongly suggest that unions of complete arcs may yield some interesting sets; the results of this paper lend some support to this claim.

References

1. E. Borós and T. Szönyi, On the sharpness of a theorem of B. Segré, *Combinatorica*, **6** (1986), 261–268.
2. A. E. Brouwer, A series of separable designs with application to pairwise orthogonal Latin squares, *Europ. J. Combinatorics*, **1** (1980), 39–41.
3. R. H. Bruck, Quadratic extensions of cyclic planes, *Proc. Symp. Appl. Math.*, **10** (1960), 15–44.
4. J. Coykendall, Half-factorial domains in quadratic fields, *J. Algebra*, **235** (2001), 417–430.
5. M. de Finis, On k-sets of type (m, n) in projective planes of square order, *Lecture Notes in Mathematics*, **49**, London Mathematical Society, 1981, pp. 98–103.
6. J. C. Fisher, J. W. P. Hirschfeld and J. A. Thas, Complete arcs in planes of square order, *Ann. Discrete Math.*, **30** (1986), 243–250.
7. J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd edn, Oxford University Press, 1998.

Received 22 January 2000 and accepted 7 November 2000
Published electronically 16 March 2001

J. Coykendall and J. Dover
Department of Mathematics,
North Dakota State University,
Fargo,
ND 58105-5075, U.S.A.